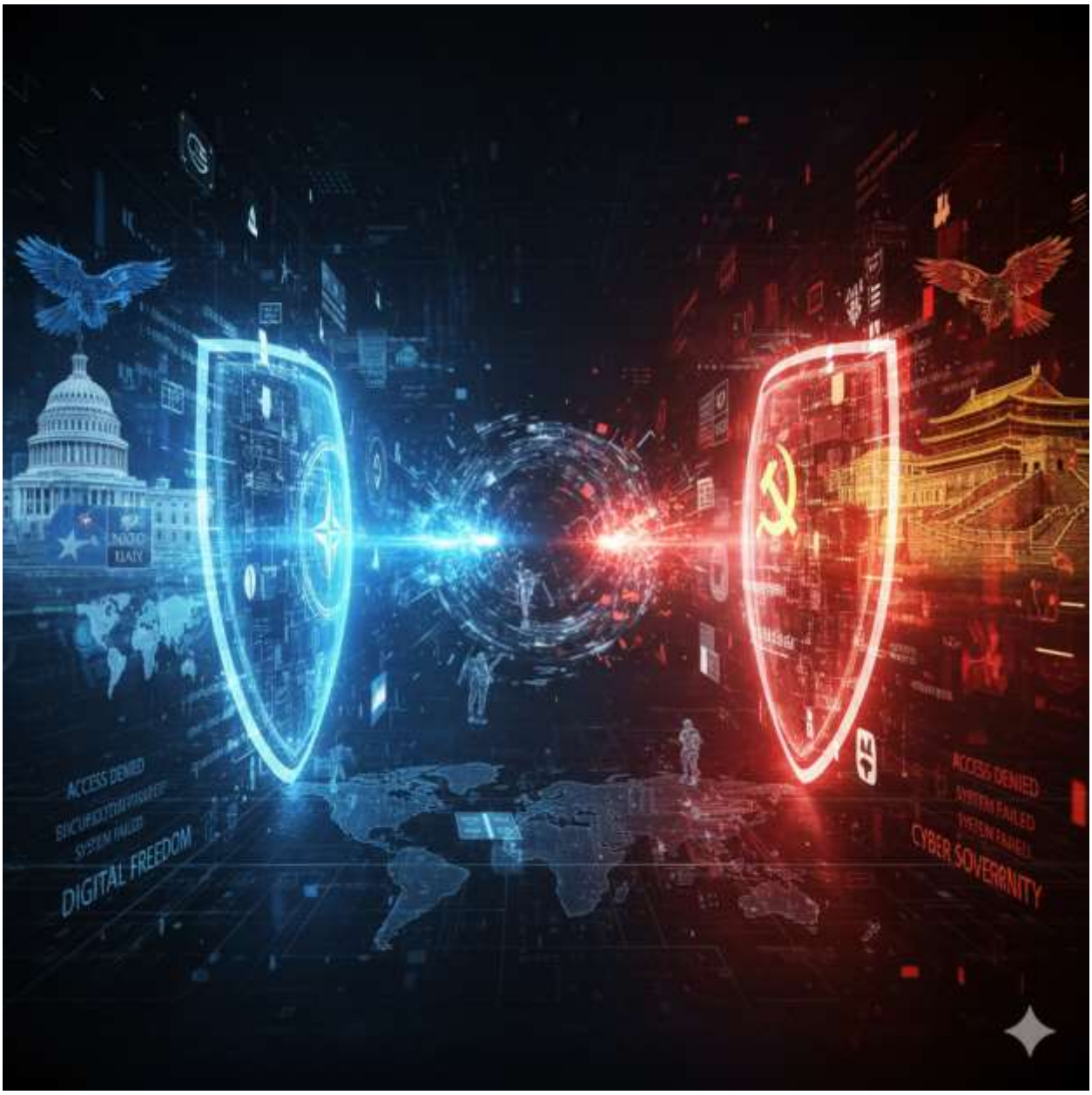
RESEARCH TITLE:

THE EAST-WEST CYBER GEOPOLITICS: HOW THE RISE OF CYBER MERCANTILISM AND THE QUEST FOR DIGITAL AUTONOMY IS POSING A CHALLENGE TO DATA AND INTERNET GOVERNANCE.

By Eliyas Kebede (LLB)

Addis Ababa, Ethiopia, August 2025


ACCESS DENIED
DIGITAL FREEDOM
ACCESS DENIED
CYBER SOVEREIGNTY

DECLARATION

I, Eliyas hereby confidently declare that this research is an original contribution to the field, reflecting my unique perspectives and independent work. Other than duly recognized and referenced statements, all expressions exclusively belong to the author except some images and terms of definitions which are generated by AI technology.

Name: _____

Signature: _____

Date: _____

ACKNOWLEDGMENT

First and foremost, to God be the glory, the ultimate source of wisdom and understanding. I am also deeply grateful to Mr. Abdulbasit Ahmed, the esteemed head of the Cyber Diplomacy Division at INSA, for his unwavering support, encouragement, and fatherly motivation.

ABSTRACT

This Research outlines a qualitative study examining the cyber geopolitical challenge to global data and internet governance posed by cyber mercantilism and the quest for digital autonomy. The research will explore the complex East-West cyber geopolitical struggle by analyzing how competing ideologies and national interests are fragmenting the global digital landscape. A qualitative research design, and desk research method will be employed. This includes analyzing preexisting researches, articles and books. I will also use a theoretical framework to decode and dissect real-world cases and events, providing new and powerful insights. This makes the research deductive qualitative desk research. This research will examine the driving forces behind the increasing trend of data localization, digital autonomy, cyber sovereignty and analyze also the diverging perspectives that are shaping global internet governance. Additionally, the research will test and refine a theoretical framework by applying its principles in the realm of techno-politics in order to analyze and explain contemporary developments in cyber politics, cyber-economics, and cyber-security, thereby contributing to the evolution of main stream theories to the realm of digital world. Finally, after examining the contemporary international cyber governance and digital geopolitics politics, this research will provide robust policy recommendations for developing countries states who are struggling to endure the intricate international cyber landscape.

Contents

DEFINITION OF TERMS, CONCEPTS, ACRONYMS AND ABBREVIATIONS 8

CHAPTER ONE: INTRODUCTION 1

PROBLEM STATEMENT 2

Cyberspace, once envisioned as an illimitable realm of collaboration, is now a vehemently contested arena where competing cyber geopolitical interests threaten its very foundation. To understand the convolutions and nitty-gritty of cyber politics and its impact on global cyber governance, this research focuses on the following precarious problems: 2

THE PURPOSE OF STUDY (OBJECTIVE) 3

General Objectives 3

Specific Objectives of the Study 3

RESEARCH QUESTIONS 4

SIGNIFICANCE OF THE STUDY 5

Practical Significance as Policy Recommendation Instrument for Developing States: 6

The significance of the research to cyber diplomacy, governance, and politics: The significance of this research, which uses pre-existing theoretical frameworks to analyze the East-West Cyber geopolitical Struggle, is substantial and multifaceted. 6

SCOPE OF THE STUDY 7

LIMITATIONS OF THE STUDY 8

ORGANIZATIONS OF THE STUDY 8

CHAPTER TWO: RESEARCH METHODOLOGY 8

Data Collection Methods 9

Document Analysis of secondary materials: This method will involve the collection and critical analysis of a wide array of preexisting researches, articles, books and other relevant documents. These will include, national cybersecurity strategies, legislative texts (e.g., China's Cybersecurity Law, Russia's Sovereign Net, EU's General Data Protection Regulation and other similar cases. 9

Data Analysis Methods 9

This research will be done through desk research method in order to save resource and time. The collected secondary data will be analyzed in light of Theoretical Framework and using Case Study methodology. 9

Justification of Qualitative Research Design 9

CHAPTER THREE: LITERATURE REVIEW 10

The East-West Cyber Geopolitical Struggle and Its Impact 11

The Concept of Cyber Mercantilism: Its Definition and Evolution 11

CHAPTER FOUR: MAJOR CYBER DEVELOPMENTS THAT SHAPED THE DYNAMICS OF GLOBAL CYBER RELATIONS 16

National Cyber Security Approaches That Redefined the Perspectives and Paradigms of Data and Internet Governance 22
CHAPTER FIVE: INTERNATIONAL CYBER RELATIONS AND CYBER DIPLOMACY 32
Theoretical Framework: 33
Conceptualizing The Intricacies of Cyber Politics in Light of Neo-Realist Perspective 34
Through The Lens of Lateral Pressure Theory 35
The Western Model of Internet Governance: A Neoliberal Project and Extension of Liberal Democracy Through the Cyberspace Globalization 36
Cyber Diplomacy and Its Subject Matter 37
Conclusion 38
Key Findings 41
Policy Recommendations for Developing States 42
What Should Be Done? 42
References 44

DEFINITION OF TERMS, CONCEPTS, ACRONYMS AND ABBREVIATIONS

Attribution: The process of identifying the perpetrator of a cyberattack.

Big Data: Extremely large datasets that may be analyzed computationally to reveal patterns, trends, and associations.

Brussels Effect: The phenomenon where a company that adheres to EU regulations applies those same standards globally.

Censorship: The practice of officially examining books, movies, etc., and suppressing unacceptable parts.

Critical Infrastructure: Systems and assets essential for the functioning of a society and economy.

Cyber Diplomacy: The use of diplomatic strategies to manage international relations in cyberspace.

Cyber Mercantilism: The use of cyber means to advance national economic interests, often at the expense of others.

Cyber Sovereignty: The idea that states have the right to govern the internet within their own borders.

Cyberspace: The digital realm of interconnected computer networks.

Data Governance: The overall management of the availability, usability, integrity, and security of data.

Data Localization: A requirement that data created within a country must be stored and processed within that country.

Data Privacy: The right of an individual to control the collection and use of their personal data.

Data Protection: The legal and technical measures used to secure personal information.

Digital Autonomy: A country's ability to control its own digital destiny without relying on foreign technologies or services.

Digital Divide: The gap between those who have access to information technology and those who do not.

DNS (Domain Name System): A hierarchical and decentralized naming system for computers, services, or any resource connected to the Internet or a private network.

Espionage: The practice of spying to obtain political and military information.

EU (European Union): A political and economic union of 27 member states located primarily in Europe.

Extraterritoriality: The application of a country's laws to activities that occur outside its borders.

Firewall: A network security system that monitors and controls incoming and outgoing network traffic.

GDPR (General Data Protection Regulation): An EU regulation on data protection and privacy for all individuals within the EU and the European Economic Area.

Global Governance: The political interaction required to solve problems that affect more than one state or region.

ICANN (Internet Corporation for Assigned Names and Numbers): A non-profit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces of the Internet.

Information Warfare: The use of information and communication technologies to gain an advantage over an opponent.

Interdependence: A relationship in which states are mutually reliant on each other.

IP Address (Internet Protocol Address): A numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.

Jurisdiction: The official power to make legal decisions and judgments.

Liberalism: A theory that emphasizes the importance of individual rights and freedoms and the role of international institutions in promoting cooperation.

Multistakeholderism: A governance model that includes participation from governments, civil society, the private sector, and other actors.

NATO (North Atlantic Treaty Organization): An intergovernmental military alliance.

Neoliberalism: A political and economic theory that favors free-market capitalism.

Neorealism: A theory that argues that international relations are driven by the anarchic structure of the international system.

Network Neutrality: The principle that Internet service providers should enable access to all content and applications regardless of the source.

Non-state actors: Individuals or groups that are not part of a government but have a significant impact on international relations.

Privacy: The state of being free from public attention.

Ransomware: A type of malicious software designed to block access to a computer system until a sum of money is paid.

Realism: A theory of international relations that emphasizes the role of the state, national interest, and power politics.

Soft Power: The ability to attract and co-opt rather than coerce.

Sovereignty: The full right and power of a governing body over itself, without any outside interference.

Splinternet: The increasing fragmentation of the internet into distinct national networks threatens to undermine the global flow of information and ideas.

Surveillance: The close observation of a person or group.

Techno-authoritarianism: A political system in which the state uses technology to monitor and control its citizens.

Techno-nationalism: The idea that a country's technological capabilities are a source of national power and security.

Telecommunications: The transmission of signs, signals, messages, words, writings, images, and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems.

UN (United Nations): An intergovernmental organization aimed at maintaining international peace and security.

CHAPTER ONE: INTRODUCTION

Cyberspace, once hailed as a utopian realm of boundless digital connection, is now a contested battleground in a growing cyber geopolitical struggle, with profound implications for the future of data and internet governance. Initially envisioned as a neutral technological innovation with the potential to foster regional and international cooperation, it has, within a short period, become one of the most politicized and weaponized instruments of competition and struggle. The rise of cyber mercantilism, states pursuing protectionist and mercantilist-oriented policies to enhance their digital autonomy is a key driver in this transformation. As states invest and display flexing of power in cyberspace, it is no longer a neutral technology, but a contested space of techno-politics, particularly among superpowers, and a domain of socio-economic and politico-military competition.

Because of its ubiquitous and ambulatory nature, the cyberspace presents unprecedented challenges to the realm of international cyber relations. The geopolitics of the cyberspace has evolved from a realm of low politics to a fiercely debated arena of high political domain. The quest for digital autonomy is rapidly growing among nation states. This voracious quest for digital autonomy is fueled by perceived vulnerabilities to external influence. In this regard, nation states are trying to protect their national digital sovereignty through protectionist cyber policy instrument. To realize the ambition of digital autonomy, cyber mercantilism has emerged as fashionable cyber security policy alternative. Even those who were the champions of free internet and data flow are rethinking their national and regional cyber policy. For instance, EU's cyber security policy has gradually shifted from regulatory capitalism to regulatory mercantilism (Farrand, B., & Carrapico, H. (2022). Now EU is asserting its digital sovereignty through regulatory cyber mercantilism. This shows us how the idea of borderless cyberspace has evolved from a global panacea to Pandora's box which heightens the East-West cyber geopolitical friction over data and internet governance, evolving from commercialization to securitization to weaponization. The rampantly raising cybercrimes and cyber warfare in the late 2000's, the Snowden revelations and Wikileaks, and the 2016 US presidential election and disinformation campaigns represent historic milestones that significantly shaped the evolution and transformation of cyberspace governance perspective. These historical developments have shaped the emergence of new ideological and conceptual arguments like digital autonomy, data localization, data

colonialism and cyber mercantilism in the sphere of international cyber governance debates. Cyber geopolitics is no abstract concept, but a tangible phenomenon with pervasive and immerse real-world consequences.

This research argues that the rise of cyber mercantilism and the quest for digital autonomy are fundamentally reshaping and redefining the realm of cyberspace governance in relation to data and internet control, exacerbating the East-West digital divide and threatening the principles of a secure, open and collaborative boundless cyberspace. To analyze this, this research explores the primary driving forces of cyber mercantilism and actors involved in the intricacies of cyber politics, by highlighting the East-West dichotomy over data and internet governance. It also examines the impact of the subject matter in international relations in general and its potential pervasive effect on developing nations in particular. This paper will give a general insight about the evolution and trajectory of world cyber politics and its influence in the global world order.

PROBLEM STATEMENT

Cyberspace, once envisioned as an illimitable realm of collaboration, is now a vehemently contested arena where competing cyber geopolitical interests threaten its very foundation. To understand the convolutions and nitty-gritty of cyber politics and its impact on global cyber governance, this research focuses on the following precarious problems:

1. Why cyberspace became an arena of competition instead of becoming an instrument of cooperation?

2. What are the primary drivers behind the increasing weaponization of cyberspace, despite its initial promise of as a borderless platform for global collaboration?

3. Is cyberspace Utopia or dystopia?

Initially envisioned as a global panacea, cyberspace has become a battleground for competing interests. As technology's scale and power have grown, it has drawn the attention of state policymakers. Henceforth, cyberspace transformed from a mere private technological realm in to sphere of economic and political influence. Now every state wants to bridle and tame the flow and development of technological advancements with in its sovereign political and legal jurisdiction.

There is diverging approaches of governance and control in relation to the cyberspace. Particularly, there is a clearly marked visible difference between the East and West in relation to data and internet governance. This has created a dichotomy of internet freedom and censorship. The proliferation of cybercrimes and state-backed espionage are the other reasons that aggravated the tension over cyber governance.

The weaponization of cyberspace is driven by multiple socio-economic and politico-military security factors. The cyberspace is not weaponized only by state actors. Both state actors and non-state actors are weaponizing it. It is a potential instrument of warfare. The idea of creating borderless cyberspace has fallen in the quagmire of cyber mercantilism. New ideas and ideals are challenging the envisioned concept of borderless cyberspace. Data localization, data colonialism, cyber sovereignty, digital autonomy and splinternet are the negations of borderless cyberspace. This puts the future of borderless cyberspace at stake.

THE PURPOSE OF STUDY (OBJECTIVE)

General Objectives

The over overarching purpose of this study is to critically examine the factors contributing to the transformation of cyberspace from potential instrument of cooperation in to an arena of geopolitical and economic competition by emphasizing on the influence of cyber mercantilism on the global cyber politics.

Specific Objectives of the Study

This study will;

1. Deeply examine the driving motives behind the rise of cyber mercantilism by navigating the economic, political and security motivations that triggered techno nationalism.
2. Evaluates the impact of cyber mercantilist policies by critically assessing the effects of data localization, digital protectionism and other relevant measures on international technological transfer and acquisition.

3. Compare and contrast competing versions of internet governance by exploring the differing approaches to internet control advocated by various nations focusing on the rising tensions between internet freedom, digital globalization, national sovereignty and security concerns.

4. Thoroughly assesses the repercussions of cyberspace fragmentation for international relations and this research will examine its pervasive implications on the erosion of cyber security trust. These objectives will be achieved through a qualitative analysis of policy documents, case studies of specific cyber governance initiatives and events. By addressing these objectives, this study will provide insights on the contemporary trending debates of cyber politics.
5. It explores the driving motives, capabilities, policies and strategies of cyber mercantilism in relation to data and internet governance, despite its initial promise as borderless platform for global collaboration. Explores the competing of visions and versions of internet governance, evaluating challenges posed by national cyber sovereignty concerns, data localization policies, digital autonomy and differing approaches to internet governance and considering the potential implications for international relations.

RESEARCH QUESTIONS

The study will address the following questions that are the bedrock of cyber governance and politics.

1. What are the key economic and political factors that have contributed to the transformation of cyberspace from a potential instrument of international cooperation in to a domain characterized by geopolitical and economic competition?

2. How the differing perspectives on cyber governance and digital autonomy are influencing the dynamics of cyberspace?
3. What are the primary drivers behind the politicization and weaponization of the cyberspace which caused conflicting view between the East and West modes and models of cyber governance?

4. To what extent is the vision of a borderless cyberspace a realistic and achievable goal, considering the competing forces of national cyber sovereignty, digital autonomy, data localization policies and the diverging approaches to internet governance among nations and what impact does it causes in the global arena?" or is the envisioned borderless cyberspace utopia or dystopia?

SIGNIFICANCE OF THE STUDY

In order to understand the global techno political development and its trajectory, it is very crucial for us to delve in to the discussion of contemporary digital actors and expressed interests in relation to global cyber politics. Understanding the global techno-political landscape is crucial for effective navigation in contemporary cyber politics, and for stakeholders to make well-calculated, rational decisions. Because uninformed or ill-informed decision maker always invites recipe for disaster. This study addresses key challenges such as:

Cyber Sovereignty: Differing interpretations of cyber sovereignty fuel international tensions and hinder the development of shared norms for responsible state behavior in cyberspace. This research analyzes competing perspectives on cyber sovereignty and cyber governance.

Digital Autonomy: The quest for digital autonomy, while intended to enhance national security and economic competitiveness, can also lead to protectionist or mercantilist policies that stifle free flow of digital technology. This study evaluates the ongoing dilemma between the East and the West in relation to cyber geopolitics and governance.

Data Localization: Data localization policies, while intended to protect user privacy and national security, can also create barriers to cross-border data flows and hinder the growth of the globalized borderless cyberspace. This research assesses the economic, political and social impacts of data localization and proposes potential alternative approaches to data governance that balance competing interests.

Data Colonialism: The growing concentration of data in the hands of a few powerful tech companies raises concerns about data colonialism, where developing countries are exploited for their data resources without receiving equitable benefits. This research examines the power

dynamics of data colonialism and proposes strategies for promoting data sovereignty and information justice.

Splinternet: The increasing fragmentation of the internet into distinct national networks threatens to undermine the global flow of information and ideas. This research explores the drivers of the splinternet and its potential outcomes.

The above elements are the most pressing challenges which became the bottleneck for borderless cyber globalization endeavors.

Practical Significance as Policy Recommendation Instrument for Developing States:

This research has profound practical significance, particularly for developing countries of Africa. After a thorough examination of contemporary international cyber governance and politics, this study will provide robust policy recommendations for African nations, particularly for Ethiopia. These recommendations will be tailored to help these countries navigate the East-West Dilemma without compromising their own development goals or digital sovereignty.

The significance of the research to cyber diplomacy, governance, and politics: The significance of this research, which uses pre-existing theoretical frameworks to analyze the East-West Cyber geopolitical Struggle, is substantial and multifaceted.

A) In Cyber

1) **Informed Negotiations:** The research can inform diplomatic negotiations by providing a clear conceptual map of the competing interests at play.
2) **Predictive Power Analysis:** By employing existing mainstream theories, the study will provide informed rational predictions about the future trajectory of cyber power relations. This equips cyber diplomats with fundamentals of international cyber geopolitical affairs.
3) **Capacity Building for Cyber Diplomats:** Serves as a training resource for diplomatic academies and Foreign Service institutions.

B) In Cyber Governance

1) **Policy Coherence:** The findings of this research and analysis definitely help cyber security institutions like INSA develop coherently comprehensive and effective national cyber governance policies.
2) **Identifying Gaps:** By navigating newly emerging realities in the realm of cyber governance and politics, this research helps to provide alternative roadmap for creating new norms, treaties and multistakeholder international and regional forums to address rising challenges.
3) **Standard Setting:** The study will contribute to the development of new international standards of cyberspace governance.

C) **In Cyber Politics**

The findings of the research will undoubtedly help to understand power dynamics of the East-West cyber geopolitical trajectory and enhances scholarly debates over the issue. This work could also lead to the emergence of a new sub-discipline which is called cyber international relations.

In nutshell, this research provides policy makers with strategic analysis of global cyber geopolitics by examining the underlining ideological fault lines that exacerbates the East-West cyber geopolitical divide. It also provides the highlights of global cyber politics and trending ideological views in relation to cyber governance. In addition to this, it will serve as steppingstone to grasp basic concepts of contemporary cyber politics like the envisioned borderless cyberspace, and digital sovereignty. It also instigates debates and further analysis in relation to developing cyber governance norms and reflected values. It paves an opening gate way for further research.

SCOPE OF THE STUDY

The scope of this research is limited to major developments of cyber governance politics of 2000s and onwards. And, the study will cover USA, EU, CHINA and RUSSIA as the main actors of East-West cyber geopolitical power struggle. Thematically, the study will address data related concepts like data localization, data colonialism, big data and concepts of cyber politics such as cyber sovereignty, digital autonomy, and cyber mercantilism.

LIMITATIONS OF THE STUDY

The research unveils only the economic, political and security aspects of the contemporary cyber governance matters. In this regard, this research doesn't deeply discuss the technical aspects of the cyber technology. Instead of examining the technical side of the cyberspace, the research focuses on analysis of the underlying interests and motives that are shaping and redefining the contemporary international cyber relations. It also roughly addresses the role of Big Tech Companies and the role of massive social media platforms such as Facebook, Google, YouTube and other similar stakeholders of the global cyberspace relations. The other shortcoming of the research is that, it doesn't take into account the current role and influence of AI technology which is profoundly challenging the contemporary ecosystem of the global cybersecurity dynamism. Particularly, the potential integration of AI technology into weapons of mass destruction. After all, there are undiscussed and unaddressed matters due to time and other constraints. In nutshell, this study doesn't encompass all the nitty- gritty of the cyberspace.

ORGANIZATIONS OF THE STUDY

The research is structured into five Chapters. The First chapter outlines introductory parts of the research such as a concise introduction of the subject matter of the study, problem statement, purpose of the study, list of research questions, significance of the research, scope and limitations of the study. The second chapter is about employed research methodology and methodological justifications. The third chapter deals with literature review and it outlines, defines and explains basic concepts of cyber politics and arguments that are fundamental to the study. The fourth chapter discusses major cybersecurity cases and national cyber policies that profoundly shaped the dynamics of contemporary global cyber relations. Finally, the fifth chapter embarks upon international cyber relations and cyber diplomacy. Key findings of the research and conclusion part are also included under this chapter.

CHAPTER TWO: RESEARCH METHODOLOGY

This chapter details the research methodology and methods that will be used to investigate "The East-West geopolitical Struggle: How the Rise of Cyber Mercantilism and the Quest for Digital Autonomy is Posing a Challenge to Data and Internet Governance." The chosen approach is a

qualitative research design, which is particularly well-suited for this complex topic, as it allows for an in-depth, interpretive, and holistic understanding of the phenomena under study.

Data Collection Methods

Document Analysis of secondary materials: This method will involve the collection and critical analysis of a wide array of preexisting researches, articles, books and other relevant documents. These will include, national cybersecurity strategies, legislative texts (e.g., China's Cybersecurity Law, Russia's Sovereign Net, EU's General Data Protection Regulation and other similar cases.

Data Analysis Methods

This research will be done through desk research method in order to save resource and time. The collected secondary data will be analyzed in light of Theoretical Framework and using Case Study methodology.

1. **Theoretical Framework:** This method is deductive research approach where collected data are interpreted in light of theoretical lenses.
2. **Case Study: the case study approach:** This study will use an instrumental case study design, where specific events are selected to gain a deeper understanding of the broader phenomenon. Cases like the European Union's regulatory regime to understand its quest for "technological sovereignty" as a challenge to both US and Chinese models. The Stuxnet worm, and the Russian malware on Estonia in 2007 will be discussed. By selecting these contrasting cases, the research can highlight the different strategies and motivations at play.

Justification of Qualitative Research Design

A qualitative research design is the most appropriate approach for this study because the core research problem is not about measuring a quantifiable relationship but about understanding a nuanced and evolving geopolitical process. It is very unwise to reduce the concepts of cyber

geopolitical debates such as digital autonomy and internet governance approaches into numerical and variables. The driving forces of cyber geological frictions are deeply rooted in political ideologies, historical contexts and strategic narratives of nation states. A qualitative design allows the researcher to explore the "how" and "why" behind these phenomena, and provides rich, descriptive insights that a quantitative approach would likely miss out (Mason, 2017).

CHAPTER THREE: LITERATURE REVIEW

Introduction

The cyber realm has come to be an arena of intense geopolitical competition and this is significantly reshaping the principles of data and internet governance. The geopolitical struggle over the cyberspace is aggravated by the rise of cyber-Mercantilism. This evolving landscape is marked by a state-centric approach that prioritizes national digital autonomy over the free flow of data and information (Nocetti, 2015). This literature review aims to dissect and analyze the ongoing East-West cyber geopolitical struggle that challenges once imagined as a borderless and decentralized cyberspace. The rising tension between multistakeholder and state centric internet governance approach has become a central theme in contemporary cyber international relations.

Conceptual Foundations

In order to have comprehensive understanding of the East-West cyberspace geopolitical struggle, it requires an examination of several key conceptual arguments that have merged in contemporary techno political debates. For instance, the concept of digital sovereignty asserts a state's right to govern its own cyberspace, including control over data stored and processed within its borders (Vatanparast, 2020). Cyber Sovereignty is manifested through data localization policies, which mandate that certain data must be kept with in a country, splinternet a direct challenge to the global interconnected nature of the internet and digital censorship that undermines freely accessible

cyberspace. This quest for digital autonomy is driven by concerns over national security, economic competitiveness and the need to protect citizens' data from foreign surveillance and exploitation. Furthermore, the literature demonstrates a move away from the traditionally envisioned borderless cyberspace understanding towards polarized views of cyberspace governance perspectives. Currently even those who were at the forefront of unrestricted internet freedom and global cyber liberalization are rethinking their policy orientations. Digital nationalism is mushrooming against digital liberalism.

The East-West Cyber Geopolitical Struggle and Its Impact

While the East champions cyber sovereignty where the internet and cyberspace are viewed as an extension of a nation state's sovereign territory, the West portrays a borderless global cyberspace which is run by multistakeholder philosophy of governance. The Eastern approach is emanated from concerns of state security and information control and this eventually causes censorship and internet fragmentation. On the other hand, the West vehemently advocates and promotes a free and open cyberspace governed by a variety of actors, including governments, civil society and private sectors. However, the emerging cyber threats and the quest for digital autonomy is creating a shift in these dynamics. The literature suggests that the very nature of these threats has led to the securitization and weaponization of cyberspace, transforming it from a domain of "low politics" (commerce and communication) to one of "high politics" (national security and military strategy) (Chatham House, 2019). The old issue aged, unresolved battle between security and freedom has reappeared in the realm of cyber politics. This literature review will synthesize existing research to highlight the underlying ideological and practical consequences of the East-West cyber friction and provides critical perspective in relation to the domain of techno politics.

The Concept of Cyber Mercantilism: Its Definition and Evolution

Mercantilism is an old endured theory of political economy that tries to balance the tension between state and market. It examines the crossroad of market and state influence. It is an arena of political economy where economy meets politics and, in this aspect, there is avenue of intersection between profit and power-driven interests. In the early days of its conception, the cyberspace was lauded as domain of boundless global interconnectedness. However, a few years later the cyber space has become a new terrain of geopolitical competition and a new policy

perspective emerged to redefine the ecosystem of international cyber relations. Cyber mercantilism is a protectionist national cyber policy that advocates digital autonomy and technological self-reliance. This paradigm represents a deliberate move by states to implement policies aimed at bolstering their national digital autonomy, often at the expense of the free flow of data and international cooperation (Deibert, 2020). The very essence of cyber mercantilism is embedded with state centric approach where the government actively intervene in the governance and regulation of digital sphere. The evolution and development of cyber mercantilism is manifested through data localization, establishment of national network, which lead to fragmentation of internet or splinternet and surfaced burning quest for digital autonomy. As Vatanparast stated, this intervention can manifest in various forms, including the imposition of data localization requirements, mandating that data generated within a nation's borders be stored and processed domestically (Vatanparast, 2020).

The drivers for the rise of cyber mercantilism are attributed to economic and political motives. Cyber mercantilism favors domestic technology over foreign originated ones and discourages foreign competition over its national digital economy. It is the mirror of classical mercantilist economic policies, where states sought to maximize exports and minimize imports in order to accumulate national wealth and power. When we come to the cyber realm, data, internet and other basic digital infrastructures are considered as strategic assets, akin to gold in classical mercantilism. The evolution of cyber mercantilism is shaped by several historical and technological developments that have redefined the global landscape of cyber geopolitics. We can indicate several historic developments that caused a shift of narration in the discourse of techno politics. For instance, the rise of cybercrime and state-sponsored cyber espionage in the 2000s exposed vulnerabilities and underscored the potential for malicious actors, both state and non-state, to exploit the interconnected nature of cyberspace and events like the Stuxnet attack and the increasing frequency of data breaches highlighted the security risks associated with an open and boundlessly ungoverned digital realm. (Carr, 2011). The 2013 Snowden revelation that unashamedly exposed the surveillance capacities of Western intelligence agencies, and the subsequent 2016 US presidential election that showed the proliferation of disinformation are among the fundamental incidents that reshaped the domain of international cyber relations. Finally, the growth of cyber mercantilism has been exalted by strategic national policies of China and Russia. The coming of the Great Firewall of China and Ru Net officially announced the beginning

of cyber mercantilism that eventually results fragmentation and polarization of the global cyberspace. Particularly China, with its Great Firewall and stringent data localization laws, have long advocated for a model of cyber sovereignty, emphasizing the right of each nation to govern its own digital space without external interference (Creemers, 2017). This inevitably invites state intervention and control in the sphere of external and internal cyber relations. We have seen the cloud of cyber capitalism policies at regional and national level in different cyber geopolitical spectrums. For instance, The European Union's shift towards regulatory mercantilism, as evidenced by GDPR and the Digital Services Act, demonstrates a move to assert digital sovereignty through robust regulatory frameworks aimed at protecting European data and promoting domestic digital industries (Sauter, 2022). The growth of cyber mercantilism has profound impact on the sacred principles of Western oriented digital perspectives such as a secure, open, and collaborative cyberspace, potentially leading to a fragmented internet, often referred to as splinternet or balkanization of internet. Policies such as data localization significantly hinder cross border data flows and this impedes the realization of borderless global cyberspace.

The prioritization of domestic technology can stifle innovation and competition in the sphere of digital economies as disheartening factor. Additionally, the divergence in national cyber policies can inevitably create regulatory complexities for multinational corporations and speedily exacerbate geopolitical tensions, contributing to an "East-West dilemma" over the future of internet governance (Nocetti, 2015). These emerging contradictions between the East-West cyber geopolitical struggle traps developing countries in the middle of competing political and economic quagmires. In order to come out from such kinds of cyber policy bottleneck, developing countries should clearly understand the contemporary global cyber political dynamics and trajectory.

The drivers cause behind cyber mercantilism are multifaceted. National security concerns and the quest for digital autonomy are catalyst of cyber mercantilism. The borderless global cyberspace poses inherent security threat to nation states. Additionally, beyond security threats, economic interests are primary instigators of protectionist state policy. In the contemporary world, data is often referred to as a strategic asset, akin to the new oil (The Economist, 2017). Nations seek to accumulate and control this resource to foster domestic innovation, bolster their own technology

industries, and gain a competitive edge in the global digital economy. Politically, some authoritarian regimes may use internet and digital power as a means of power consolidation and propaganda dissemination. In this regard, the government may be tempted to limit free flow of information. Digital dictatorship is an emerging contemporary cyber political discourse. So, political cause is another driving force for the development cyber mercantilism and rise of techno nationalism. In nutshell, the contemporary global cyberspace dynamics is full of competing and conflicting interests and this puts the dream of borderless digital world at stake.

The Limitations of Existing Research on Cyber Politics Particularly on The East West Techno Power Competition for Cyberspace Leadership

The existing research on the East-West techno power struggle for cyberspace leadership suffers from fundamental limitations. The shortcomings of past scholarship include fragmented theoretical approach and it fails to recognize cyberspace as an extension of historical rivalries, an underestimation of the ideological clash at the heart of the conflict, and an overly optimistic, and now demonstrably flawed, utopian view of a borderless digital world.

1. The Absence of a Comprehensive and Consolidated Theoretical Framework

The previous researches over emphasis on security securitized aspects of the cyberspace landscape. It was always discussed from security perspective. Some scholars, has viewed the field through the lenses of neorealist perspectives. While this is a critical component, it is insufficient to fully capture the picture of the global cyber geopolitical landscape. Because the underlying cause of the East-West cyber geopolitical struggle are trans-security factors like ideological justifications. Volumes of pre-existing researches portrayed and examined the intricacies of cyberspace matters in light of securitization theory. I can say that, the cyberspace was over securitized and less politicized and rarely ideologicalized as well.

2. The Fallacy of Novelty: Cyberspace as a Continuation of History

The other most significant limitation of the past researches is that, the cyberspace politics was considered as a wholly novel phenomenon, detached from the enduring currents of political and

economic history. This kind of perspective wrongly portrays the East-West cyber geopolitical struggle as a new form conflict, rather than being considered as continuation of long-standing ideological rivalries. The cyberspace is a new invention that is meant to serve the old purpose. The contemporary strategic competition for dominance in cyberspace is a direct echo of traditional great power struggles over land, sea, and air. In this regard, failure to recognize these historical continuities, that many works have missed the deeper, structural drivers of the conflict, instead focusing on tactical cyber security skirmishes and technological developments as if they were disconnected from the broader geopolitical context.

3. The Overlooked Ideological Dimension: Nationalism vs. Globalization

There was ideological underestimation of the values that underpin cyber political debates. Security threat was considered as primary driver, and the fundamental clash of nationalism versus globalization has been unduly neglected. The East-West cyber geopolitical dilemma mirrors a battle of competing philosophies. On one side, a liberalist envisioned, a global borderless, open internet as a force for free trade, information, and democratic values. On the other side, a more nationalistic perspective prioritizes state control, social stability, and cultural sovereignty. This ideological chasm explains why nations like China and Russia invest heavily in digital autonomy and strict internet control. The issues of cyber politics are therefore more than just securitization and economization; they are a manifestation of a profound ideological struggle over the very future of human organization.

4. The Collapse of the Cyber-Utopian Narrative

Lastly, much of the foundational research on cyber international relation and politics suffered from a naive cyber-utopianism that optimistically envisioned borderless cyberspace. A number of early influential authors were overly optimistic about the potential of a boundless cyberspace as a globalizing and democratizing force that fosters values of liberalism. Many Authors like John Perry Barlow, in his 1996 Declaration of the Independence of Cyberspace, boldly declared that governments had no control over the digital realm. His work, along with that of others like Nicholas Negroponte, optimistically championed a future of decentralized digital power, painted

a picture of a cyber-utopia where information would be universally free and borders would become impossible (Negroponte, 1995). However, this overly optimistic declaration has been utterly dismantled and shattered by the realities of state-sponsored surveillance, data localization laws, and the construction of digital firewalls and contradictory internet governance approaches. The west envisioned boundless cyberspace and this has given way to digital dystopia where the same technology once lauded as a tool for liberation has become a potent instrument for state control, digital tyranny, surveillance, information and cyber warfare.

CHAPTER FOUR: MAJOR CYBER DEVELOPMENTS THAT SHAPED THE DYNAMICS OF GLOBAL CYBER RELATIONS

Prominent Cyber Security Cases That Exacerbated the East-West Cyber Geopolitical Friction

1. The September 2024 Mossad's Cyber Operation Against Hezbollah's Military Communication Gadgets

In 2024 the Mossad of Israel conducted historic cyber operation against Hezbollah's thousands of pagers and walkie-talkies in Lebanon and Syria. It marks the dawn of very advanced evolution of modern cyberwarfare. The traditional cyber operation heavily relies on remote hacking and stealing high value data or information. The operation has significant repercussion on the global digital security confidence building. It erodes the trust between the technology supply chain and end users. It undoubtedly casts shadow of mistrust between and among technology companies, governments and end user customers. The 2024 cyber operation reminds us how cyberwarfare is dangerously advancing from time to time. The weaponization of the cyberspace is blurring the lines between digital and physical attacks. The Mossad targeted the supplier of pagers and walkies-talkies of Hezbollah through remote triggering and synchronization and amazingly caused explosion. This kind of operation deteriorates security trust on electronic devices. This gives stark warning and forces us to conclude in alarming tone by saying no technology is safe. It causes global doubt about the transparency and security of electronic device manufacturers and suppliers. The global cybersecurity ecosystem is facing paramount mistrust and doubt. Later or soon cases like the 2024 Mossad's operation inevitably causes erosion of cyber security trust in the supply

chain. It shatters the believe of secure and transparent global technology supply chain. It compromises the security and integrity of electronic devices. The infiltration of Israeli government in the supply chain of technology sends alarming message to the international cyber security ecosystem. It also poses a complex question in relation to corporate responsibility and liability. It raises critical questions like who should be liable, how, why and to what extent? It also complicates attribution of cyber-attacks. It impacts the presumed neutrality of technology companies.

In this regard, technology companies may no longer be considered as mere profit seeker business establishments, but as dangerously powerful techno political entities. Gradually we will see balkanization of technology and this leads increased scrutiny of foreign made technologies. It fuels already developing cyber mercantilist sentiment among nations and favors domestic manufacturers for critical infrastructures and government use. Countries will be forced to develop their own separate technology and this what is called balkanization and fragmentation of the cyber tech ecosystem.

In nutshell, the 2024 Mossad's deadliest cyber-attack signals a stark warning about the complexity and viciousness of rapidly advancing modern cyberwarfare. I can say that this sort of operation irreparably erodes the global cybersecurity trust among nation states and digital business conglomerates.

2. The Stuxnet: The Dawn of a Digital Weapon

Discovered in 2010, and believed to be a joint cyber warfare project of USA and Israel. It targeted Iran's nuclear digital facilities. Initially the Stuxnet aimed to destroy the Natanz Uranium enrichment facility. Later on, it also used to steal secret data. This malware was designed to harm high value industrial computers. The Stuxnet worm subtly alters the frequency of the industrial control systems and it also simultaneously fed false data to the operators, making it appear as though everything was running normally, thereby delaying detection for months. (Zetter, 2014).

The Stuxnet was historic development that heralded the beginning of cyberwarfare. For the first time, cyber operation has grown from a mere espionage to causing disruption and physical harm. This shows us how digital weapon can cause immense damage on the adversary's infrastructure. In addition to intelligence gathering, cyber-attack is capable of causing physical harm. The Stuxnet paved a new chapter for state sponsored digital warfare.

3. The Not Petya: The Uncontrolled Cyber Weapon

This incident originated from Russia's military intelligence in 2017. The malware caused unintended and unforeseen digital disaster. In the cybersecurity ecosystem the incident showed us how uncontrolled malware results unforeseen cyber catastrophe. Its primary target was Ukraine. It was deployed through a compromised Ukrainian accounting software (M.E. Doc CISA, 2017). It caused over 10 billion economic losses to several

multinational corporations like Maersk and FedEx. The malware unforeseeably surpassed its initial purpose and caused devastating collateral damage. Its initial goal was to cripple Ukraine, but its wild nature became unmanageably difficult to control. So, unleashing a devastating malware may not be easy to control. Sometimes, certain cyber warfare malwares may open Pandora's box exceeding their intended purpose and causes catastrophic malware-pandemics.

4. **The Titan Rain: As Digital Warfare of Espionage**

The Titan Rain was Chinese CCP affiliated cyberwarfare instrument. Happened from 2003-2006 and was orchestrated for cyber espionage purpose. It targeted US computers selectively targeting government agencies and defense contractors, including NASA and Lockheed with the goal of stealing sensitive classified information related to military and aerospace technology (Daggan, 2010). Its persistent duration teaches us that, a malware can pose consistent threat and harm. Even after its discovery, the Titan Rain has managed to stay for years significantly threatening the global cyber security paradigms.

5. **The Black Energy**

It was orchestrated against Ukraine's power grid. Aimed to cause power outage and it affected hundreds of thousands of people (Booz Allen Hamiton, 2016). It was the first cyber-attack that targeted power grid infrastructure and successfully caused a power outage proving that the digital sabotage could directly impact a population's daily life and national cyber security. It announced a new phase of cyberwarfare and ensured the ability to wage a cyber-physical attack. A cyber warfare produces tangible physical harm causing visible damage by invisible digital weapons.

Unlike conventional weapon, the cyber weapon is too dynamic and subtle. The cyber warfare is also difficult to predict. In fact, the cyberwarfare paradigm is full of subtlety and flexibility. As the world digitalization rapidly grows from time to time, the cyber weapons will become more devastating not less than nuclear weapons. From the defender's perspective, cyber warfare is difficult to predict and defend. Without roaring of guns, only a keyboard click can destroy a nation. It is a weapon of mass crippling.

6. The 2007 Cyber Attack on Estonia

It was the landmark case in the history of modern cyberwarfare. The Russian originated ransomware crippled the Estonian digital infrastructures. Estonia was the pioneer of rapid digitalization and e-government. However, the incident shows us, without formidable and sustainable cyber security assurance, rapid digitalization is recipe for cybersecurity disaster. Following the attack, in 2008 NATO members recognized the gravity of the matter and established cooperative cyber defense center of excellence (CCDCOC). NATO members also incorporated cyber-attack as an act of war that potentially triggers Article 5 which invokes collective self-defense.

National Cyber Security Approaches That Redefined the Perspectives and Paradigms of Data and Internet Governance

1. The Emergence of Russia's Ru Net and Its Implication on the Western Multi-stakeholder Model of Internet Governance

On February 28, 2022 the ministry of digital transformation of Ukraine sent a letter to ICANN which is the global authority for internet domains and the Ukrainian government requested to cut Russia's ru.net domain from the global web. A few days later three of world's biggest companies allowing internet traffic flow in and outside Russia announced that they would drop their Russian client from the global internet system. Russia has been decoupling its domestic networks from the global internet since 2019 when it enacted its so-called sovereign internet law and on the 6th of March the Kremlin claimed successful disconnection from the global internet.

Technically speaking, the Russian Ru Net passed five levels of disconnection from the global internet. Firstly, at domain level, secondly disconnection of cross border internet traffic, thirdly at application level, fourthly disconnection from the global network at cloud services and finally

disconnection at content level. ICANN is western affiliated private organization that administers global network domains and IP addresses. In this regard, it has created reasonable doubt particularly on the East and global south digital world.

The emergence of Ru Net (Russia's Sovereign National Internet) marks a milestone development in the history of global internet governance. Russia has developed its own independently operable national sovereign network. This ignites already existing climate of mistrust and uncertainty in the cyber ecosystem. Ru Net poses a direct challenge to the multi stakeholder model of internet governance which is championed by the western nations. The Russian state controlled national sovereign network negates the western model of internet governance. It excludes the civil society and private actors. The government is the sole decision maker. This marks a dramatic shift from multi-stakeholderism to statecentrism. This effectively replaces the global cooperative model with a statecentric one, prioritizing national security and control over the principles of an open internet (Epifanova,2020). This puts the dream of having open internet at open stake. The quest for digital autonomy is not a mere slogan of totalitarian regimes. Rather it is a commonly shared vision of both democrat and totalitarian governments. The need to have independent, secured and nationally controlled digital infrastructure doesn't necessarily entail the desires of authoritarian regimes. It is about creating independent, sustainable, and secured digital assets in order to enhance the cybersecurity of citizens.

The Ru Net officially heralded the beginning of splinternet and erosion of interoperability. The era of internet fragmentation is ahead of us. We will see more isolated national networks. Unfortunately, the very strength of internet lies in its interoperability and the emergence of isolated national networks profoundly impacts the global internet governance. Gradually the legitimacy and power of ICANN is diminishing. The Ukrainian attempt to cut off Russia's Internet domain from the global network signaled bad omen to the western model of multi-stakeholder internet governance which is predominantly run by ICANN.

In nutshell, Russia's voracious quest for digital autonomy stets a formidable precedent that casts eternal repercussions on the future of the western backed multi-stakeholder version of internet governance which is anchored upon the sacred digital principles like open, neutral and free internet access. The Ru Net is the direct negation and anti-thesis of theses western oriented principles.

2. The Chinese Great Firewall: The Digital Shield of CCP

In the early days of internet era, there was international optimism about spread of democratic values through cyber liberalization. It was well established vision of democratic leaders of the west. The west strongly envisioned that, internet will be the agent of anti-totalitarian virus. President Bill Clinton of US said that, there is no question that China has been trying to crackdown on the internet …good luck …that is a sort of like trying to nail the Jell-O to the wall. He thought that, containing internet will be impossible. According to his perspective the transformation of Chinese political system via internet power was a foregone conclusion. In the beginning, an internet was considered as inherent agent of democracy. Because of the open and decentralized nature of internet, it was said to be the internet bears elements of global democratization. Despite commonly held vision to use internet as instrument of democratization and freedom of information, internet censorship emerged to falsify the vision of cyber democracy.

The Chinese Communist Party adopted the Great Fire Wall of its own and disproved the commonly visioned cyber utopia. The emergence of the Great Firewall has profound impact on the future of internet governance. The Great Firewall is a multi-layered and multi purposed digital shield orchestrated to control and monitor internet and information flow from within and outside of Chinese digital borders. It is one of the largest internet censorship tools. It employs IP blocking and deep packet inspection which scans data packets for key words and phrases which are

politically sensitive. It also has legal instrument that forces foreign tech companies to comply with its censorship demands. For instance, the cybersecurity law centralizes all internet policy and requires companies to register users under their real names and to immediately stop the transmission of banned content (Freedom House, 2018). It is a tool for maintaining social and political control by preventing the dissemination of information deemed a threat to national security or the stability of the CCP such as contents about human rights, pro-democracy movements, the Tiananmen Square Protests, and other historical events that challenge the party's narrative (The Guardian, 2018). By doing this, the CCP can easily disseminate its own version of truth and political propaganda. This system has also had the secondary effect of fostering a domestic internet industry, as blocked foreign companies like Google, Facebook, and X the former Twitter are replaced by state sanctioned alternatives such as Baidu, WeChat, and Weibo, which operate under strict government supervision (Britannica, n.d).

A) The Great Firewall as The Negation of Cyber Democratization

Now internet is no more unstoppable **instrument of democratization.** China has managed to nail Jell-O to the wall. Previously it was said to be technology will make it increasingly difficult for the state to control the information its people receive …the Goliath of totalitarianism will be brought down by the David of the microchip (Ronald Reagan, Speech at Guildhall, June 14, 1989). This was the popular thinking of the time. President George W. Bush and Bill Clinton believed internet as inherent force of democratization. The Internet was considered as a political weapon. Walter Wriston has argued in Foreign Affairs that, "the virus of freedom" …is spread by electronic networks to the four corners of the Earth," and Robert Wright claims that "in all probability, resistance to the internet's political logic will plainly be futile in a decade. John Perry (the cyber guru) also predicted the same scenario. It was the conventional wisdom of early 1990's. An assumption that portrays internet as inherently the nemesis of tyranny is a black box reasoning. An internet is equal friend of freedom and tyranny as the same time. Now China has built its own version of internet and the ambition of democratization through the cyberspace has failed from realization. China has successfully nailed Jell-O to the wall. Contrary to the conventional wisdom of the early 1900's, China is using internet to fight democracy. Cyber resistance against democracy is very possible and highly likely. Now we are witnessing counter democratization in the digital

realm. China's experience with great firewall demonstrates how considering internet as inherent force of democratization was naïve. Some individuals attempted to circumvent the system using Virtual Private Networks (VPNs), the government has responded with sophisticated counter measures, cracking down on unauthorized VPN services and targeting users who attempted to breach the firewall (Journal of Democracy, 2017). Activists and Journalists who have used the internet to expose corruption or criticize the government have faced severe legal repercussions, including long prison sentences (Freedom, House, 2021). A 2009 study by Xiaoru Wang concluded that, the internet is "unlikely to offer democratic hope for China, at least not in the near future," as its mobilizing effects are constrained by censorship and rising nationalistic sentiments (Wang, 2009).

B) The Repercussions of the Great Firewall on Internet Governance and Freedom

The emergence of the Chinese Great Firewall marks the birth of digital authoritarianism. The Chinese Digital Silk Road Project has opened a new paradigm in cyber politics and internet governance. Through this project China provides technology and financial incentives to other nations, particularly authoritarian regimes, to adopt similar systems of centralized internet control (Tech Policy. Press,2025) It poses a formidable challenge on the multistakeholder model of internet governance and cyber liberalization. The Chinese Great Firewall and Digital Silk Road Project have become a bottleneck and quagmire for the global cyber ecosystem. Very soon the Chinese model of internet governance will be adopted by numerous likeminded states.

3. The EU's General Data Protection Regulation (GDPR) as the Pioneer of Cyber Mercantilism

The GDPR is one of the most important legal and policy instruments of European data governance. Its main purpose is to protect and secure personal data of EU citizens and nationals. This shows us how the issue of data governance has become a pivotal matter with in European cyberspace. The GDPR is not a mere policy instrument of citizen's private data protection. It also has the ambition of ensuring competitive advantage of European digital economy. EU is moving from regulatory

capitalism to regulatory mercantilist cyber policy. This happened based on the EU's perceived loss of economic competitiveness, high degree of dependence on foreign digital infrastructures and service providers and threat of cyber security. Bearing in mind that, a considerable percentage of technological infrastructures are under private control EU seeks to reassert its control over cyberspace, impose digital borders, accumulate data wealth and reduce its dependence on external private sectors whose values may not reflect those of the EU order (Farrand, B., & Carrapico, H. (2022). A new approach is emerging in which the non-EU private sectors can be considered as much as a threat as foreign powers and from whom digital sovereignty must be secured. This shows as a shift of EU's policy in relation to cyber governance.

Previously EU's cyber policy was regulatory capitalism particularly when it comes to in public-private cyber security and governance relations. However, recently these relations with the private sector are being reconceptualized. Now EU is rethinking its past cyber policy. While the domestic private sectors are being regulated through steering and rowing, the foreign private sectors are however are considered as economic competitors and potential agents of other states (Farrand, B., & Carrapico, H. (2022). They are considered as a threat to the cyber security of EU's geopolitical domain. EU wants to strengthen the Union's digital sovereignty in order to face the economic and security challenges of the twenty-first century (Von der Leyen, 2021a). EU as a new comer in the debates of digital sovereignty, it understands the concept of digital sovereignty as an ability to act independently in the digital world (Madiega, 2020, p.1). This idea of independence doesn't exclude domestic private sectors. However, it tries to regulate and control foreign tech companies that doesn't share the visions and values of EU in relation to cyber policy governance. EU wants to welcome only likeminded foreign private sectors into its cyberspace. EU is increasingly making distinctions between EU based companies which adheres to its values and non-EU large tech companies. In order to understand the current cyber mercantilist policy of EU, Farrand, B., & Carrapico, H. have classified the evolution of capitalist as follows;

1. The 1st stage was Laissez Fair capitalism (1800-1930's) characterized by steering and rowing which advocates minimum state interference.
2. The second phase is called welfare capitalism (1940's-1970) invites calculated and systematically regulated state intervention.

3. The third level was the era of regulatory capitalism which lasted from 1980-2010.
4. And, now the fifth phase of capitalism which is known as Networked Regulatory Capitalism is on the service (2010-).

In order to address the shortcomings of regulatory capitalism, regulatory mercantilism has emerged as new fashionable cyber policy alternative. Regulatory mercantilism tries to balance the tension between state and market. There is a perpetual struggle between profit seeker private sectors and power maximizer state actors. The market is driven by profit and the state motivated by power. And, this is called political economy an arena of intersection where the economy meets the politics.

In its general notion, mercantilism prioritize a positive trade balance in which imports where restricted and exports were promoted (Allen, 1991). Currently a neo mercantilism has emerged as strategic trade protectionism and government economic activism to promote state wealth and power including the realm of cyber economy and cyber politics. Where the international relation is preoccupied with realist conceptions of sovereignty, the EU's own sovereignty turn is not surprising (Farrand, B., & Carrapico, H. (2022). Russia-Ukraine war and the rise of China's influence have contributed for EU's cyber policy shift. USA based social media platforms were increasingly being used to spread disinformation and destabilize European democracies both in the context of the UK's referendum on EU membership and national elections (Morgan, 2018 and Hameleers, 2020). These kinds of incidents directly triggered the quest for digital autonomy within the European cyber geopolitics. It is not too late to achieve technological sovereignty in some critical technology areas (Von der Leyen, 2019, p.13). During the Von der Leyen Commission digital sovereignty was defined as an ability to choose a European way for digital technologies, balancing the opportunities presented by the use of data with privacy, security, safety and ethical standards. Reducing dependency on the other parts of the globe particularly on US based companies like Facebook or Google and Chinese HUWAWEI is potential threat to EU's network infrastructure (Farrand, B., & Carrapico, H. (2022). The changing relations between foreign based Big Tech Companies and EU cybersecurity aims are made really apparent in the cybersecurity strategy for the digital decade published in December 2020 and EU is thinking global and acting European (European

Commission and High Representative of the Union for Foreign Affairs and Security Policy 2020, p.4). According to the commission, EU envisages three important values in the arena of cyber governance like leadership, resilience, and technological sovereignty. Amazingly, USA and China alone host more than 80% of the World's data (Aktoudianakis,2020, p.4). Furthermore, it is estimated that while 92% of the data produced in the West is hosted in the USA, only 4% is hosted in the EU (Kalft and Renda, 2019, p. 173). Now the era of cyber sovereignty has come and the state is about to reshape and redefine the relations in the digital realm. The EU's GDPR has a visible cloud of cyber mercantilist policy ingredients. EU is trying to achieve the realization of DIGITA AUTONOMY through implicit and subtle data localization policy mechanisms. The GDPR has extra territorial applicability and it sets standards and also prescribes penalties for non-compliance. This is called the Brussel effect.

The extra territorial applicability of the GDPR triggers the question and concept of data colonialism. In contemporary cyber politics, data colonialism is one of the most contentious emerging techno political concepts. Data has become the newly discovered gold in the blue sky. Without doubt, I can wholeheartedly say that, data will be the fuel of the third WORLD WAR. And, this new gold needs new policy governance and perspective. That is why the EU adopted a comprehensive data regulation policy which is called the GDPR. So, the EU wants to ensure its digital supremacy through protectionist cyber policy instrument. The GDPR of EU is a clear manifestation of mercantilist cyber policy. EU is determined to protect its digital economy from external non-EU competitors. In this regard, the GDPR creates immense pressure on emerging digital economies. Developing digital economies will struggle a lot to meet the EU's GDPR standard. Startup tech companies will face significant legal and technical havocs. The GDPR is the shield of European digital economy. It provides legal and technical defense for European cyber ecosystem. As a result, the GDPR acts as a protective measure for the EU's internal market, shielding it from external competition and reinforcing its digital sovereignty (Budnitsky, 2022). Particularly this creates a considerable havoc on emerging digital economies.

EU's Implicit Data Localization Policy and Its Implications

EU has adopted subtle data localization policy. According to Chapter 5 of the GDPR data can be transferred outside the EU if the destination country provides an adequate level of protection or if appropriate safeguards are in place (European Union, GDPR, Article 45). But the question is what kind of protection level is said to be adequate? By default, adequate level of protection means the same data regulation policy that the EU has envisaged in its GDPR. For that matter, the European Commission is in charge of determining adequacy of data protection laws and policies. In this regard, the decision on a country's data protection efficiency and adequacy is the subject of cyber geopolitical discussion.

The take it or leave it approach of EU's GDPR is a clear manifestation of data localization. EU has a monopolistic and protectionist cyber policy in relation to data regulation. The GDPR is not a mere legal or policy instrument. Rather it is a weapon orchestrated against EU's digital economy competitor. EU wants to establish standards of international data governance. The GDPR has foiled Eurocentric data governance approach. As I mentioned it earlier, the GDPR sets significant encumbrance on emerging digital economies. It sets obstacles for developing digital economies from forging their own national or regional alternative ways in the realm of cyber economy.

The Impact of the GDPR on Internet Freedom and Free Flow of Information

The GDPR has introduced some controversial principles with in the ambit of personal data protection policy framework. One of the contested provisions is the right to be forgotten. This has raised concerns that it could be used to suppress information including journalistic content and historic records (European Union, 2018). The high cost of compliance also negatively affects free flow of information. It seems EU is gradually negating its own long standing envisioned principles such as internet freedom, diversity, free flow of information and equitable access. It shades shadow on EU's diversity of digital market. Costs associated with GDPR's compliance leads to more monopolized digital landscape dominated by a few tech companies reducing competition in the digital market ecosystems.

In its face value, the GDPR seems highly positive and individual-centric digital security protection framework. However, it is embedded with mercantilistic and discriminatory policy

orientations and it has wide range of political and economic ramifications in the realm of the international digital market. In the guise of protecting citizens' personal data, the EU has successfully established defensive digital economic policy. The GDPR has also introduced defacto data localization policy that can have multifaceted impacts on the global digital geopolitical landscape.

CHAPTER FIVE: INTERNATIONAL CYBER RELATIONS AND CYBER DIPLOMACY

A new portfolio has been incorporated in the realms of international relations. The cyberspace has emerged evolved from the subject matter of low politics to the most sensitive and highly debated arena of high politics. Particularly the emergence of fiercely debated concepts like cyber sovereignty and digital autonomy vividly revealed the rising techno political struggle among nation states. In this regard, cyber politics is posing paramount challenge to the old power dynamics of international system, directly challenging mainstream foreign policy theories. Now the modern system is in dual struggle between the Real and Virtual World. This is the time, where a man claims, asserts, and establishes identity and his rights, interests and ambitions on the virtual world.

Historically, the scope and focus of international relation evolved from state-centric to non-state actors and furthermore the contemporary international relations has incorporated techno-centric perspective. This shows us how the current international relation is influenced by technological developments like the cyberspace technology which significantly reshaped the global power dynamics. Now a days, the cyberspace technology has become instrument of perusing power and wealth. A new form of imperialism is under formation. The cyberspace technology is no more a mere realm of economic gain, but it has become instrument of power struggle. According to Lass Well's political equation, the study of politics is who gets what, when and how. And, this political algebra is equally applicable in the domain of techno politics. The study of politics is the study of influence and influential (Harold Lass Well, 1958). So, without doubt I can say that, technology is

one of the most influential domains in the sphere of international relations. This has also caused the emergence of techno political discourse. Today it is very difficult to identify an arena of politics that is devoid of cyber related manifestations (Nazli, 2012). Cyber politics has created the dichotomy of global brains and global bodies. Richard N. Rosecrans's "The Rise of Virtual State" (1999), the traditional power domains are replaced by brain power (Nazli, 2012). Currently the synergy between technology and politics has become unbreakably everlasting bond.

Previously, in the common parlance, cyber space was considered as the negation of state sovereignty. But in the contemporary understanding, the cyberspace redefined and reshaped the notion of sovereignty instead of negating it. Jack Goldsmith and Tim Wu (2006, p. 58) reminded us that the internet is not unbound with respect to geography and that specific technical norms operate to reinforce the foundations of that we consider sovereign boundaries and this includes the usual directives of choose a country or choose a server. In this regard, the proverbial Pandora's box of competing interests and powerful contentions threatens to spring open and seriously undermine the 21st century understanding of structures and processes in international relations (Nazli, 2012).

Theoretical Framework:

Why Theoretical Framework Becomes Indispensable to Grasp the Intricacies of Cyber International Relations

The rapidly evolving cyberspace has launched a new complex dimension to the international affairs. In modern day world, digital technology profoundly shapes interactions between nation states. In order to move beyond mere description and to cultivate meaningful analysis, a theoretical framework is fundamentally important. Theoretical perspectives provide a lens through which we interpret events, identify patterns and present predictions. Theories serve as fundamental tool for both scholars and policy makers wrestling with the trials of international cyber relations.

Conceptualizing The Intricacies of Cyber Politics in Light of Neo-Realist Perspective

Accord to the realist framework, the international landscape is a self-help system. So, states must struggle to ensure their existence and wellbeing. The cyberspace is the extension of traditional geopolitical arena. Basically, neo-realism portrays the international system as anarchial arena of power struggle among nation states. In this case, state actors bitterly struggle in order to accumulate power and wealth in every possible dimension as much they can. The unapologetically anarchial nature of the international system inevitably ignites the quest for digital sovereignty and autonomy. Henceforth, the pursuit of digital autonomy is a rational and predictable response in order to ensure the survival of the fittest. Power struggle that has been for millennia in the physical world is mirrored in the digital realm. The ongoing power struggle among nations over the leadership of cyberspace is the extension of traditional geopolitics. Now the cyberspace has become a new domain for power struggle. The emergence of the Chinese Great Firewall and Ru Net of Russia is the manifestation of the heightening geopolitical power struggle in the sphere of cyber technology. States are inherently power seekers and maximizers. In fact, it is the inherent nature of and business of state actors to pursue power and wealth. That is why the global system is always full of competition and struggle. The cyber access and use can be legitimately be characterized as chaotic, reinforcing global anarchy.

In recent years, the policy deliberations surrounding cyber security in the United States have become increasingly politicized, involving diverse government agencies, private contractors and consultants through the various mechanism by which decisions are made and assume an alternative nature, notably with respect to the allocation of resources required (Nazli, 2012). For, instance we can mention deliberations made to ban TikTok. And the EU's rush for digital autonomy is another indication of neo-realist response to the perceived vulnerability and a desire to balance the power of the US and China in the digital sphere (Mayer & Lu, 2022). In nutshell, interdependence and over reliance on foreign technology in the unabashedly anarchial system creates a loophole for vulnerability and because of this reason, states will be tempted to maximize their own national wealth and power in relation to digital technology.

Through The Lens of Lateral Pressure Theory

Lateral Pressure argues that, the pressure that comes out of population size, lack of sufficient natural resources and other issues of national interest, impudently pushes states to exert power and influence outside their sovereign domain. According to this theory, states are tempted to exercise their power outside their territorial boundary. In this respect, the cyberspace technology becomes invaluable choice for state actors to project their national interest outside of their boundary. The driving force behind this push is generally attributed to lack of strategic natural resources. Digital resources like Big Data are the modern replica of gold and silver. Particularly, those who are deprived of natural resources, resort to the cyberspace technology. Because it provides a much better strategical alternative. The driving logic in lateral pressure theory is rooted in the volume and nature of human demands, needs, wants, desires, claims and counter claims and the ways in which societies seek to meet the demands and we must now recognize, homo cybricus has emerged, whose creation is a function of cyberspace and whose persona may be either economicus or politicus (Nazli, 2012). Accordingly, I can say that, historically a mankind has evolved from a mere social animal to homo economicus and politicus and finally to homo-cybricus.

Latera pressure theory best explains the underlying elements and nature of cyber politics because the theory has adopted comprehensive and multilayered methods of analysis. It takes in to account the role of private sectors and perceives the ecosystem of cyber politics as synergy of private sectors, civil society and the public domain. Each actor is motivated by its own respective interest. And this makes the domain of cyber politics an arena of intersection where profit, freedom, and power struggle against each other.

The Western Model of Internet Governance: A Neoliberal Project and Extension of Liberal Democracy Through the Cyberspace Globalization

The neo liberalist lens with its optimistic view focuses on cooperation, international institutions and the role of no-state actors. Despite the anarchial nature of the international system, liberalists envision an opportunity for cooperation.

Following the dismantlement of the Soviet Union, the political philosopher Francis Fukuyama in a superlative fashion declared "the end of history." He boldly argued that, the ideological struggle between the East and West had concluded with the triumph of liberal democracy and free market capitalism (Fukuyama, 1992). This thesis optimistically dreamed a future of multifaceted convergence, where all nations would gradually adopt a single, universal political and economic order. Unfortunately, decades later the thesis of global liberal democracy and capitalism was shattered by the resurgence and re-emergence of super power competition. In this respect contrary to the contemplated success of globalist liberal democracy, democratic backsliding started to occur.

After the physical world showed stiff resistance and resilience to a uni-polar global order, the cyber space was considered as the last resort for the project of globalization. Initially, it was assumed that, the cyberspace, with its borderless nature and decentralized architecture, was optimistically seen as the last alternative hope for the realization of the globalist liberal democracy. The fall of the Berlin Wall and the disintegration of the Soviet Union in 1991 seemed to be a prove for the Fukuyama's eulogy.

Fukuyama's predictive wishful thinking has been reversed and now we are not witnessing the end of history, rather we are living through the beginning of history. The rise of China as a formidable economic and geopolitical power and also, the historic re-emergence and come back of Russia under Vladmir Putin has presented a robust model of state-led economy and heavy-handed alternative of governance. Likewise, internal democratic backlash and populism with in the western democracies revealed deep seated vulnerabilities for the success of liberal democracy. And, the cyberspace technology becomes the last resort as we approach the end of history itself. As the physical world become a more difficult theatre for the project of globalization, attention shifted to cyberspace.

The multi-stakeholder moder of internet governance bears the inherent political values of the western beyond its economic logic. Free and open internet has an instrumental vale for the projection and spread of democratic cultures across the globe. The internet's open architecture such as the principle of "end-to-end" design, is seen as inherently conducive to freedom of expression and political dissent. This allows individuals to organize against dictatorship without state censorship. This narrative usually described as cybernetic exceptionalism which portrays the internet as a unique space that transcends national borders (Goldsmith & Wu, 2006). This is in line with the traditions of liberal democracy that applauds and exalts individual rights and freedoms.

In Light of Constructivism

Gives emphasis on the role of ideas, norms, and shared identities and this aspect its orientation of analysis shifts from material power to shared values. In this context, the cyberspace geopolitical struggle should be explained in light of the very meanings of cyber-attacks, cyber espionage, cyber warfare, data colonialism, cyber sovereignty and digital autonomy. Whether a certain cyber action is considered cyber-crime, an act of espionage or an act of cyber warfare depends on the shared beliefs and norms of the international community. Particularly, this framework is important in order to understand the concepts of cyber sovereignty and digital autonomy and why different states hold varying interpretations. The very debates of cyberspace geopolitics emanate from meanings and interpretations.

Cyber Diplomacy and Its Subject Matter

Cyber diplomacy is a new portfolio in the realm of international relations. As cyber security and governance emerge as a new dynamism of international affairs, cyber diplomacy surfaced to create common understanding, reduce risk and improve stability. Cyber diplomacy involves private sectors, civil societies and public domain. Cyber diplomacy is a new addendum to the field of international relations and foreign policies. Cyber diplomacy strives to create responsible state behavior and non-state bearing habits. Unfortunately, the world of cyber diplomacy is full of mistrust and competition. Every state aspires to be a digital hegemonic power. Because of challenges posed by cyber security realm, it is said to be technology is eating foreign policy. Cyber

diplomacy is relatively young field of international relations. Cyber diplomacy is the art of bridging technology and politics. The environment of cyber diplomacy is shaped by super powers. They are the norm setters. Cyber security and digitalization are shaking international norms established during 1945. In this regard, the golden verses of international relations and laws need to be redefined and reinterpreted. New techno political concepts are surfacing. The cyber world is a new defying and defining factor in modern international relations. A cyber diplomat must be equipped with better understanding of the international cyber power relations and dynamism. In its general algebraic equation, cyber diplomacy revolves around questions of who wants what, why and how? A cyber diplomats should identify and clarify one's own interests and also must know other's demand, and finally choosing the best possible modus operandi is called the art of diplomacy.

Conclusion

The contemporary cyberspace geopolitical struggle has paved new conceptual and practical dimension in relation to internet and data governance. The cyberspace has become one of fiercely debated arenas of political and economic struggle. The reasons that caused the cyberspace, as domain of competition instead of an instrument of cooperation are attributed to several reasons.

a) **The first and foremost reason is attributed to political cause.** This less navigated cause. Because even the very perception of perceived security threat is influenced and preceded by deeply entrenched underlying preconceptions of political ideologies. Everything is defined and redefined by political preconception.

There are underlying competing ideological motives behind the rising cyber geopolitical struggle between the East and West in the sphere of digital world. Particularly newly emerged techno political concepts like digital autonomy and sovereignty are profoundly aggravated the geopolitical tension of the cyberspace. Ideological clashes and conflict of interests have caused differing and rival models of data and internet governance. This is the fundamental cause for the contemporary emerging digital divide.

The second cause comes out of economic rational. From this perspective the digital realm, as a new lucrative opportunity of trade, inevitably invites economic competition. There is economic struggle between liberalist market-led and mercantilist state-regulated models of digital economic systems that eventually caused the rise of cyber-mercantilism. In this aspect, the economic competition of digital economy has a dual dimension. This happens internally or at national level between public and private sectors, and externally at international level among nation states (inter-governmental level).

The third and the obvious reason is associated with securitization. Even though this is the overly discussed and overestimated cause, it can be the other significant factors of digital divide. For some states, the boundless nature of the cyberspace is considered as a source of vulnerability. Amazingly, now adays, even those who were the champions of borderless cyberspace are rethinking their policy orientations. States are resorting to cyber mercantilism in order to avert the influence of the so-called unfriendly states with in their sovereign political and economic domain.

Why weaponization of the Cyberspace?

The increasing weaponization of the cyberspace emanates from multiple components.

1. **Geopolitical Tensions:**

The preexisting geopolitical struggle among superpowers has been extended to the realm of digital world via the power of cyberspace technology. The ongoing struggle over the cyberspace leadership is the extension of traditional geopolitical struggle which was conventionally undergoing for the control of rimland and heartland. Now who rules the cyberspace commands the whole world. That is why we are observing immense battle for the hegemonic supremacy of global cyberspace leadership and digital technology.

2. **The Interconnected System of the Cyberspace Creates Perceived Fear of Vulnerability.**

The interconnected digital system potentially opens fertile opportunity for malicious cyber-attack. This causes perpetual fear of perceived fear of vulnerability. It also erodes trust among stakeholders in the realm of cyber security.

3. The Absence of Consolidated Legal System

The cyber legal regime is poorly developed domain of international law. The cyber legal regime is highly contested and less consolidated compared to other fields of international laws. Particularly, there is considerable legal lacuna in relation to attribution of cyber-attack. This has become the bone of contention and unresolved subject matter. An attempt has been made to assimilate and transplant the principles of other domains of international laws into the cyber realm. But, because of the unique and ambulatory nature of the cyberspace technology, these kinds of transportive endeavors stuffer considerable technical and conceptual limitations.

4. Ramification of Cyber crimes

Increasingly sophisticated and highly advanced modern-day cyber-crimes and non-state and state backed cyber-attacks aggravates the weaponization of the system. This will happen for defensive and offensive reasons. For instance, cases like the 2024 Mossad's cyber operation against Hezbollah's military communication devices signals alarming development in the cyber security ecosystem. In this particular case, Mossad targeted the supply chain of the technology in order to harm the end user. This shows significant shift from the old model of cyber-attack. Furthermore, this fundamentally erodes the already fractured trust with in the stakeholders of the cyber security ecosystem. In nutshell, these are the primary driving reason d'etre behind the rapidly increasing weaponization of the cyberspace technology.

On the other hand, the vision to create boundless global cyberspace has become a dystopia. The contemporary cyberspace governance is policy fragmentations. As the success of globalization and the wave of liberal democracy gradually recedes, the vision of borderless cyberspace project is also falling apart in parallel. Cyber nationalism and regionalism are emerging to counter the expansion and the success of cyber globalization. Splinternet, data localization, data colonialism, digital autonomy and cyber sovereignty are the negations of boundless global cyberspace. It is a foregone conclusion that, we are moving away from envisioned cyber utopia to the real and inevitable cyber dystopia which reflects the actual and inevitable power struggle of mankind.

Key Findings

b) The dynamics of the global cyberspace is shifting from Western oriented trajectory to an arena of multi polar influence. The Western digital dominance is gradually dwindling. As a result, the cyberspace geopolitical struggle will increasingly grow and inevitably creates permanent digital divide.

c) Unpredictably and rapidly advancing cyberwarfare is creating perceived fear of vulnerabilities. And, this is eroding security trust building endeavors among the stakeholders of cyber security ecosystem.

d) Previously, the cyberspace technology was presented and analyzed from security perspective and it was over securitized and less politicized subject matter. However, in present-day cyberspace relations, the cyberspace has evolved from a domain of low politics to fiercely debated arena of high political cause. As I have said earlier, even the perception of security is influenced and preceded by preconceptions of political ideologies. Everything is defined and redefined by political preconception.

e) The vision to create boundless global cyberspace is sandwiched in the quagmire of digital fragmentations. Currently, seeds of digital divide are mushrooming. And, the battle between cyber globalization and emerging techno-nationalism inevitably creates perpetual digital rift. Cyber authoritarianism is another force which is emerging to counter the wave of globalist liberal democracy.

f) Cyber geopolitics is an extension of existing political, ideological and economic rivalries that are deep-seated in history. The cyberspace is a new technology that serves the old needs of mankind. Technology rarely invents new interests, rather it is meant to best serve the old desires of humanity.

Policy Recommendations for Developing States

Digital Autonomy as A Must and Limits of Comparative Advantage

In the common parlance, as long as you have money and comparative advantage, buying foreign technology seems the short cut. And according to the economic rational of comparative advantage, nations benefit by specializing in the production of goods and services in which they have a lower cost and then trading for others. However, Technological sovereignty particularly digital technological sovereignty has strategic imperative. Unlike other consumer goods or raw materials, technology is not a mere consumable commodity. Due to its inherent strategic value, the deep integration of digital technology into critical infrastructures causes considerable multifaceted vulnerabilities. Therefore, the quest for production of domestic technology is not a mere economic choice but a strategic necessity for overall national wellbeing. Particularly this is very indispensable policy consideration for developing nations.

What Should Be Done?

1. **Building Foundational and Critical Digital Infrastructure**

   Developing countries should prioritize investing in critical digital infrastructures. Overreliance on foreign-owned infrastructure can create vulnerabilities and limit a nation's ability to control its own digital destiny.

2. **Establish National Data Centers:** To address data localization and digital sovereignty, governments should incentivize or build national data centers to store and process citizens' and government data locally. This reduces dependence on foreign cloud providers and ensures data remains under domestic jurisdiction.

3. **Adopting Comprehensive Legal and Regulatory Frameworks**

All-encompassing and consolidated legal frameworks are essential for establishing digital sovereignty and combating data colonialism. This can be done by implementing Comprehensive Data Protection Laws like EU's General Data Protection Regulation (GDPR) and enacting a Digital Sovereignty Act which allows the state to regulate its own digital matter by its own.

4. **Fostering a Domestic Technology Ecosystem Though Local Tech Start-ups Promotion Incentives:** Governments can provide incentives, grants, and tax breaks to local tech companies specializing in cybersecurity, software development, and hardware manufacturing.
5. **Actively Engaging in Global Governance**
   While pursuing digital autonomy, developing countries should not isolate themselves and entertain non-aligned cyber foreign policy. They must actively participate in international forums to shape the future of cyber governance and ensure their voices are heard.
6. **Forming Regional Alliances with Like Minded States:** Regional cooperation can amplify the influence of developing nations. Creating regional data-sharing agreements and cybersecurity pacts can help countries collectively bargain with large technology companies and respond to cross-border cyber threats.
7. **Adopting Proportional Pace of Digitalization:** Avoiding rapid digitalization without having formidable cyber security assurance.

References

1. Aaronson, S. A. (2017). What Are We Talking About When We Discuss Digital Protectionism? The George Washington University IIEP Working Paper Series, 2017-9.

2. Aktoudianakis, E. (2020). "EU Defence Package: Defence Procurement and Intra-Community Transfers Directives." European Parliamentary Research Service Study. European Parliament. Retrieved from https://www.iris-france.org/wp-content/uploads/2020/10/EPRS_STU2020654171_EN.pdf

3. Al-Jazeera. (2024, September 18). Hezbollah walkie-talkies exploded too, what to know about Israel's attacks. Retrieved from https://www.aljazeera.com/news/2024/9/18/more-devices-exploding-across-lebanon-whats-happening

4. Allen, W. R. (1991). "Mercantilism Revisited." *Journal of Economic History*, 51(1), 1-28.

5. Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation. Retrieved from https://www.eff.org/cyberspace-independence.

6. Bollow, N. (2014). Western-dominated Internet governance harms Southern economies. *Third World Resurgence*, 287/288.

7. Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27-40.

8. Bradford, A. (2023). *Digital Empires: The Global Battle to Regulate Technology*. Oxford University Press.

9. *Britannica*. (n.d.). Great Firewall. Retrieved from https://www.britannica.com/topic/Great-Firewall

10. Brookings Institution. (2016). *Multistakeholder Internet governance: A pathway completed, the road ahead*. Retrieved from https://www.brookings.edu/wp-content/uploads/2016/06/multistakeholder-1.pdf

11. Budnitsky, A. (2022). "The Authoritarian Tech-Scape: Digital Repression and Techno-Nationalism in Russia." *Journal of Democracy*, 33(4), 102-116.

12. Budnitsky, S. (2022). A relational approach to digital sovereignty: E-Estonia between Russia and the west. *International Journal of Communication*, 16, 1918–1939.

13. Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publishers.

14. Carnegie Moscow Center. (2019). Russia's Sovereign Internet Law Will Kill Innovation. Retrieved from https://carnegie.ru/commentary/78946

15. Carr, J. (2011). *Cyber shock: Why the warning signs are being ignored--and what we can do to avert disaster*. Overlook Press.

16. Center for Strategic and International Studies (CSIS). (2025, April 14). The Limits of Chip Export Controls in Meeting the China Challenge. https://www.csis.org/analysis/limits-chip-export-controls-meeting-china-challenge

17. Centre for International Governance Innovation (CIGI). (2025). *The Digital Silk Road and China's Influence on Standard Setting*. No. 264.

18. Chatham House. (2019). *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention*. Retrieved from https://www.chathamhouse.org/

19. Choucri, N. (2012). *Cyberpolitics in International Relations*. The MIT Press.

20. Cloudflare. (2024). Navigating data localization and compliance. Cloudflare.

21. Couldry, N., & Mejias, U. A. (2019). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press.

22. Creemers, R. (2017). Cyber sovereignty in China: The struggle between control and autonomy. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 7(6), e1224.

23. Deibert, R. J. (2020). *Reset: Reclaiming the internet for civil society*. House of Anansi Press.

24. Deibert, R. (2013). *Black Code: Inside the Battle for Cyberspace*. Signal.

25. DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.

26. Denzin, N. K. (1978). *The research act: A theoretical introduction to sociological methods*. Aldine.

27. Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, 14(4), 532-550.

28. Epifanova, A. (2020). Deciphering Russia's "Sovereign Internet Law". German Council on Foreign Relations. Retrieved from https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law

29. European Commission and High Representative of the Union for Foreign Affairs and Security Policy. (2020). *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade*. JOIN(2020) 18 final. Brussels: European Commission. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020JC0018

30. European Parliament. (2024). The global reach of the EU's approach to digital transformation. Retrieved from https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2024)757632

31. European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

32. European Union. (2018). Questions and Answers – General Data Protection Regulation. European Commission.

33. Farrand, B., & Carrapico, H. (2022). "Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity." *European Security*, 31(4), 481-504. https://doi.org/10.1080/09662839.2022.2102896

34. Freedom House. (2018). The Rise of Digital Authoritarianism. Retrieved from https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

35. Freedom House. (2021). China: Freedom on the Net 2021 Country Report. Retrieved from https://freedomhouse.org/country/china/freedom-net/2021

36. Freedom House. (2024). Freedom on the Net 2024: Russia. Retrieved from https://freedomhouse.org/country/russia/freedom-net/2024

37. Fukuyama, F. (1992). *The End of History and the Last Man*. Free Press.

38. Gilpin, R. (1987). *The Political Economy of International Relations*. Princeton University Press.

39. Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet?: Illusions of a Borderless World*. Oxford University Press.

40. Google search results from a query on "2024 Mossad operation against Hezbollah communication devices", "how cyber attacks are used as a weapon", and "impact of cyber warfare on cybersecurity trust among technology companies." (2024, September). Multiple sources including Wikipedia, AP News, and CBS News.

41. Gurstein, M. (2014). The multistakeholder model and neoliberalism. *Third World Network*, 287/288.

42. Hameleers, M. (2020). "Populist Disinformation: Exploring Intersections between Online Populism and Disinformation in the US and the Netherlands." *Politics and Governance*, 8(1), 195–204. https://doi.org/10.17645/pag.v8i1.2478

43. Harvey, D. (2005). *A Brief History of Neoliberalism*. Oxford University Press.

44. Herzog, S. (2012). "Revisiting the Estonian Cyber Attacks: Digital Threats and Multination". *Journal of Strategic Security*, 4(2).

45. Journal of Democracy. (2017). The Road to Digital Unfreedom: President Xi's Surveillance State. Retrieved from https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-president-xis-surveillance-state/

46. Kalft, A., & Renda, A. (2019). "Data, Cloud Computing, and the EU Digital Single Market: A New Frontier for Competition Law and Policy." In M. Botta, W. Kerber, & A. P. D. F. Renda (Eds.), *Competition Law and Economics: European Perspectives on Competition Law and Policy* (pp. 165-188). Edward Elgar Publishing.

47. Keohane, R. O., & Nye, J. S. (1977). *Power and Interdependence: World Politics in Transition*. Little, Brown.

48. Kwet, M. (2019). Digital colonialism: The United States' empire of technology and its global strategy for domination. Monthly Review Press.

49. Life of Soldiers. (2025, February 20). The Digital Silk Road: Implication Of China's Techno-Political Strategy. https://www.lifeofsoldiers.com/2025/02/20/the-digital-silk-road-implication-of-chinas-techno-political-strategy/

50. Lyon, D. (2015). *Surveillance after Snowden*. Polity Press.

51. Madiega, T. (2020). "Digital sovereignty for Europe." European Parliamentary Research Service Briefing. European Parliament. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646173/EPRS_BRI(2020)646173_EN.pdf

52. Mannion, C. (2021). Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets. *Vanderbilt Journal of Transnational Law*, 53(2), 685.

53. Mason, J. (2017). *Qualitative researching*. Sage publications.

54. Mayer, M., & Lu, Y. (2022). Digital Autonomy? Measuring the Global Digital Dependence Structure. ResearchGate.

55. Meltzer, J., & Pearson, C. (2024). How is innovation competition exacerbating global overcapacity? Bruegel.

56. Mondo. (2025). The EU Digital Services ACT (DSA): Implications for the US. https://mondo.com/insights/eu-digital-services-act-impact-implications/

57. Morgan, G. (2018). "Online disinformation and the EU's response." European Parliamentary Research Service Briefing. European Parliament. Retrieved from https://www.europarl.europa.eu/RegData/etudes/ATAG/2018/620230/EPRS_ATA(2018)620230_EN.pdf

58. Mueller, M. (2010). *Networks and States: The Global Politics of Internet Governance*. MIT Press.

59. Mueller, M. L. (2017). Will the internet fragment? Sovereignty, globalization and cyberspace. Polity Press.

60. Mueller, M. (2017). The Metamorphosis of Internet Governance. In *The Politics of Internet Governance* (pp. 11-30). Oxford University Press.

61. Musiani, F. (2022). Reassessing “infrastructuring digital sovereignty”: digital self-determination as a set of infrastructure-embedded practices. *Frontiers in Communication*.

62. NATO. (n.d.). Cyber defence. Retrieved from https://www.nato.int/cps/en/natohq/topics_78170.htm

63. NATO Strategic Communications Centre of Excellence. (2008). 2007 cyber attacks on Estonia. Retrieved from https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf

64. Negroponte, N. (1995). *Being Digital*. Alfred A. Knopf.

65. Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs*, 91(1), 111-130.

66. Organski, A. F. K., & Kugler, J. (1980). *The War Ledger*. University of Chicago Press.

67. Ottis, R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. CCDCOE.

68. Pohle, J., & Thiel, T. (2020). The return of the state: a political economy of digital sovereignty in Europe. *Internet Policy Review*.

69. ResearchGate. (2020). China's Conception of Cyber Sovereignty: Rhetoric and Realization. Retrieved from https://www.researchgate.net/publication/339680028_China's_Conception_of_Cyber_Sovereignty_Rhetoric_and_Realization

70. Sauter, M. (2022). Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity. *East European Politics*, 38(4), 589-609.

71. Stadnik, K. (2019). Sovereign Runet. Internet Governance Project. Retrieved from https://www.internetgovernance.org/wp-content/uploads/IGPWhitePaper_STADNIK_RUNET-1.pdf

72. TechPolicy.Press. (2025). How China Governs Its Internet and Plans to Export Its Model. Retrieved from https://www.techpolicy.press/how-china-governs-its-internet-and-plans-to-export-its-model/

73. The Economist. (2017, May 6). The world's most valuable resource is no longer oil, but data. *The Economist*.

74. The Guardian. (2018). The great firewall of China: Xi Jinping's internet shutdown. Retrieved from https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

75. The Guardian. (2024, September 19). Israeli front-controlled manufacturing process likeliest explanation for attacks on Hezbollah. Retrieved from https://www.theguardian.com/world/2024/sep/19/israeli-front-controlled-manufacturing-process-likeliest-explanation-for-attacks-on-hezbollah

76. Vatanparast, M. (2020). Data governance and the elasticity of sovereignty. *Brooklyn Journal of International Law*, 46(1), 1-50.

77. Von der Leyen, U. (2019). "A Union that strives for more: My agenda for Europe." Political Guidelines for the Next European Commission 2019–2024. European Commission. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_19_4274

78. Waltz, K. N. (1979). *Theory of International Politics*. McGraw-Hill.

79. Wang, X. (2009). Behind the Great Firewall: The Internet and Democratization in China. University of Michigan. Retrieved from https://deepblue.lib.umich.edu/handle/2027.42/64681

80. Wendt, A. (1999). *Social Theory of International Politics*. Cambridge University Press.

81. Wikipedia. (n.d.). 2007 cyberattacks on Estonia. Retrieved from https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

82. Wikipedia. (2024). Sovereign Internet Law. https://en.wikipedia.org/wiki/Sovereign_Internet_Law

83. Wilson Center. (2022). Why Trust Matters in Supply Chains. Retrieved from https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/SC_220809_Why%20trust%20matters%20REPORT%20V1r2.pdf

84. Yanow, D. (2006). Thinking qualitatively: The "hows" of qualitative research. In D. Yanow & P. Schwartz-Shea (Eds.), *Interpretation and method: Empirical research methods and the interpretive turn* (pp. 5-27). M.E. Sharpe.

85. Yin, R. K. (2009). *Case study research: Design and methods*. Sage publications.